DOD Secure Cloud Computing Architecture

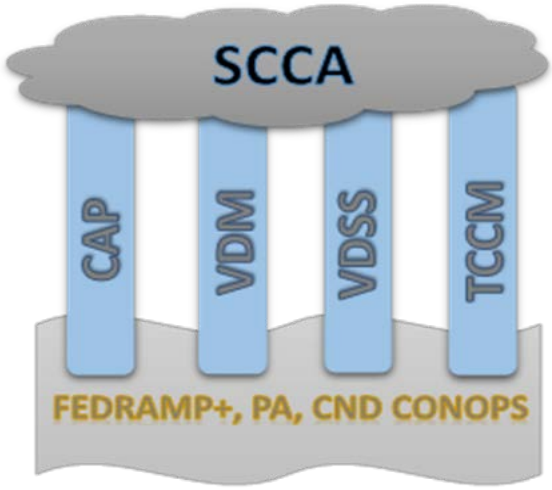
A Scalable, Cost-Effective Approach to Securing Cloud-Based Programs Under a Common Security Architecture

Overview

DISA's Secure Cloud Computing Architecture (SCCA) is DISA's approach to transition legacy systems to the commercial cloud. Based on the DOD Cloud Computing Security Requirement Guide (CCSRG), the SCCA leverages the FedRAMP+ process for Cloud Service Provider (CSP) provisional authorization.

SCCA includes four components to address cloud network and data security:

- Cloud Access Point
- Virtual Data Center Security Stack
- Virtual Data Center Managed Services
- Trusted Cloud Credential Manager



SCCA Features

Cloud Access Point (CAP) w/MeetMe CSP Connection Point: Provides access to the cloud and protects the Defense Information Systems Network (DISN) from the cloud. Provides break and inspect, intrusion detection, and Full Package Capture (FPC) to support Boundary Cyber Defense (BCD) and interface translations necessary for cloud service offering (CSO) compatibility.

Virtual Data Center Security Stack (VDSS): Enforces virtual network enclave security; provides perimeter and infrastructure network defense services as the central peering point within a mission owner's cloud environment. VDSS is essential to Mission Cyber Defense (MCD) in the cloud.

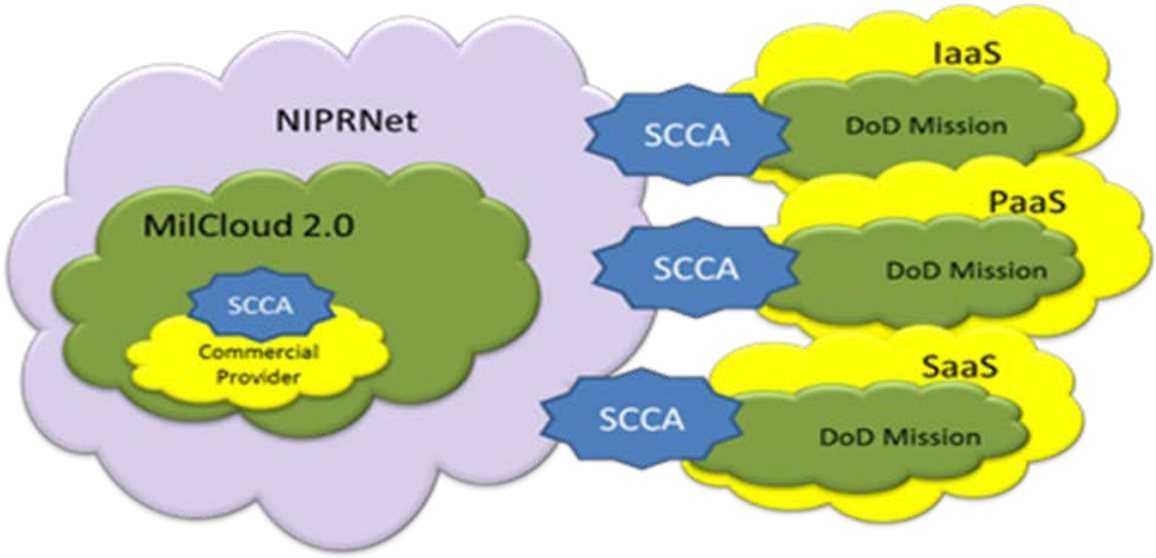
Virtual Data Center Managed Services (VDMS): Provides application host security to include Host Based Security Service/Assured Compliance Assessment Solution (HBSS/ACAS), Gold Images, patching, configuration management, identify and access, and other management services.

Trusted Cloud Credential Manager (TCCM): An individual or organization that becomes the single holder of root credentials CSP user accounts. This role is appointed or assigned by the mission owner authorizing official (AO).

DOD Secure Cloud Computing Architecture

SCCA Scope and Capabilities

The SCCA is designed to cover all aspects of commercial provider implementation. It addresses the security concerns inherent in today's industry offerings for Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). Additionally, It includes support for both on premise and off premise commercial providers.



On the Horizon

- Continue current NIPRNet Federated Gateway support as the Interim CAP (10G web content filter (WCF) capacity and three MeetMe locations).
- Collect industry SCCA functional requirements documentation (FRD) responses.
- Evaluate the feasibility and cost of moving the CAP capabilities to the MeetMe CSP Connection Point.
- Establish SCCA Testbed for research and development purposes.
- Start SCCA Pilot in FY17.

Industry Partner Engagement

- Technical Exchange Meeting – Targeted for May 2016.
- SCCA FRD comments due June 1, 2016.

Contact Us

DOD Cloud Services Program

Email: disa.meade.sd.mbx.scca@mail.mil